IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants:	Raikar et al.	Patent Application	
Serial No.:	10/632,446	Group Art Unit:	2143
Filed:	July 31, 2003	Examiner:	Shin, Kyung H.

For: CONFIGURING SECURE TEMPLATES FOR AN APPLICATION AND NETWORK MANAGEMENT SYSTEM

Appeal Brief

Table of Contents

Real Party in Interest

The assignee of the present invention is Hewlett-Packard Company.

Related Appeals and Interferences

There are no related appeals or interferences known to the Appellant.

Status of Claims

Claims 1-19 remain pending. Claims 1-19 have been rejected. This appeal involves Claims 1-19.

Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Action has not been filed.

Summary of Claimed Subject Matter

Independent Claims 1, 8 and 14 of the instant application serial no. 10/632,446 pertain to various embodiments for configuring secure templates for an application and network management system.

Independent Claim 1 recites, "A method (300, Figure 3) for configuring templates." This embodiment is described at least at page 1 lines 20-35; page 2 lines 14-30; page 3 lines 4-17; page 8 line 15 to page 9 line 32; page 11 lines 16-18; and Figures 2-3. "Configuring a template (T1, Figure 2) for an application and network management system (201, Figure 2) with first information (instruction 1, Table 1 on page 30) for determining whether data associated with at least one message received by the template (T1, Figure 2) should or should not be processed by the template (T1, Figure 2)" is described at least at page 31 lines 4-25; and 302, Figures 2-3. "Configuring the template (T1, Figure 2) with second information (instructions 2 and 3, Table 1 on page 30) for processing the data associated with at least one of the received messages," is described at least at page 31 lines 4-25; 302, Figure 2; and Figure 3. "Configuring the template (T1, Figure 2) with third information (instruction 4, Table 1 on page 30) for preventing the communication of at least one received message to other templates (T3, Figure 2) of the application and network management system (201, Figure 2)," is described at least at page 32 lines 1-8; 306, Figure 2; and Figure 3.

Independent Claim 14 recites, "A computer system (190, Figure 1) comprising: a memory unit (104, 102, Figure 1); and a processor (101, Figure 1) coupled to the memory unit (104, 102, Figure 1), wherein the processor (101, Figure 1) executes instructions associated with a template automator (292, Figure 2), and wherein the instructions of the template automator (292, Figure 2) are for:" This embodiment is described at least at 292, Figure 2; page 1 lines 20-35; page 2 lines 14-30; page 3 lines 4-17; page 8 line 15 to page 9 line 32; page 11 lines 16-18; and Figures 1-3. "Configuring a template (T1, Figure 2) for an application and network management system (201, Figure 2) with first information (instruction 1, Table 1 on page 30) for determining whether data associated with at least one message received by the template (T1, Figure 2) should or should not be processed by the template (T1, Figure 2)" is described at least at page 31 lines 4-25; and 302, Figures 2-3. "Configuring the template (T1, Figure 2) with second information (instructions 2 and 3, Table 1 on page 30) for processing the data associated with at least one of the received messages," is described at least at page 31 lines 4-25; 302, Figure 2; and Figure 3. "Configuring the template (T1, Figure 2) with third information (instruction 4, Table 1 on page 30) for preventing the communication of at least one received message to other templates (T3, Figure 2) of the application and network management system (201, Figure 2)," is described at least at page 32 lines 1-8; 306, Figure 2; and Figure 3.

Independent Claim 8 recites, "A method for providing a guideline to developers for creating templates, the guideline comprising information used by the developers for." This embodiment is described at least at page 9 lines 1-3; page 1 lines 20-35; page 2 lines 14-30; page 3 lines 4-17; page 8 line 15 to page 9 line 32; page 11 lines 16-18; and Figures 2-3. "Receiving first information (instruction 1, Table 1 on page 30) entered by a developer to configure a template (T1, Figure 2) of an application and network management system (201, Figure 2) for determining whether data associated with at least one message received by the template (T1, Figure 2) should or should not be processed by the template (T1, Figure 2)," is described at least at page 31 lines 4-25; and 302, Figure 3. "Receiving second information (instructions 2 and 3, Table 1 on page 30) entered by the developer to configure the template (T1, Figure 2) to process the data associated with at least one of the received messages," is described at least at page 31 lines 27-36; 304, Figure 3; and Figure 2. "Receiving third information (T1, Figure 2) entered by the developer to configure the template (T1, Figure 2) to prevent the communication of at least one received message to other templates (T3, Figure 2) of the application and network management system (201, Figure 2)," is described at least at page 32 lines 1-8; and 306, Figure 2; and Figure 3.

Appellants respectfully point out that according to the embodiments recited by independent Claims 1, 8 and 14 the first information, the second information and the third information are all associated with the same template.

Grounds of Rejection to be Reviewed on Appeal

1. Claims 1-7 and 14-19 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application Publication no. 20030188189 by Desai et al. (referred to herein as "Desai").

2. Claims 8-13 are rejected under 35 U.S.C. §103(a) as being unpatentable over Desai in view of U.S. Patent No. 6,957,348 by Flowers et al. (referred to herein as "Flowers").

Arguments

1. Whether Claims 1-7 and 14-19 are anticipated under 35 U.S.C. 102(e) by Desai (20030188189)

Appellants have reviewed the cited art and respectfully submit that the embodiments as recited in Claims 1-7 and 14-19 are not anticipated by Desai in view of the following rationale.

> MPEP §2131 provides:
> “A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). … “The identical invention must be shown in as complete detail as is contained in the ... claim.” *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

A. Cited Art does not show the Identical Invention

Claim 1 recites,

> A method for configuring templates, the method comprising:
> configuring <u>a template</u> for an application and network management system with first information for determining whether data associated with at least one message received by <u>the template</u> should or should not be processed by <u>the template</u>;
> configuring <u>the template</u> with second information for processing the data associated with at least one of the received messages; and
> configuring <u>the template</u> with third information for preventing the communication of at least one received message to <u>other templates</u> of the application and network management system. (emphasis added)

Appellants respectfully submit that Desai does not teach or suggest any of the features recited by Claim 1.

Appellants understand Desai to teach a method and a system for detecting intrusions that involves correlating events to improve the quality of generated alarms based on log information that is collected by devices associated with the Internet as services are requested and provided over the internet. More specifically, Appellants understand Desai to teach the following: Copies of logs are made at devices that for example request Internet services (paragraphs 0043-0046 and Figures 3-4). The copies of the logs are sent and collected on a centralized server in order to analyze and correlate these log copies. Filtering techniques are used as a part of analyzing the copied logs to determine traffic patterns (Figure 5). Further, filtering techniques are used to reduce the number of alarms and to increase the quality of alarms that result from analyzing/correlating the copied logs. Thresholds are applied as part of the filtering techniques to determine traffic patterns. Processing of requests may be modified depending on the result of the traffic pattern determinations (paragraph 0077).

Appellants understand Desai to refer to <u>templates</u> and classes interchangeably as a part of his <u>filtering techniques</u> (paragraphs 0022, 0023, 0054-0061). For example, Appellants understand Desai to refer to templates for identifying log based abnormal behavior and identifying knowledge based attack signatures (0022, 0023). Appellants understand Desai to discuss filters for quantifying data and comparing the findings (0054) and to classes as a part of identifying traffic patterns (0055-0061).

Referring to Figure 5, Appellants understand Desai's event correlation engine processing (59) to be performed <u>after</u> Desai's thresholds and filters are applied (55). Although, Desai does not explicitly disclose that Desai's filters/templates always process Desai's logs, Appellants believe that it is an inherent feature of Desai's filters/templates to always process Desai's logs because if Desai's filters/templates (55) did not always process all of Desai's logs, Desai's logs would not be available for correlation (59) in order to reduce duplicate or false alarms, among other things. Therefore, Appellants respectfully submit that Desai fails to teach “configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template,” (emphasis added) as recited by Claim 1.

Appellants do not understand Desai to teach that the same one of Desai’s filter/template can be configured with “…first information for determining whether data associated with at least one message…should or should not be processed…,” “…second information for processing the data associated with at least one of the received messages…” and “…third information for preventing the communication of at least one received message to other templates…” as recited by Claim 1, as will become more evident.

Appellants do not understand Desai to teach a filter/template that includes “third information” for preventing the communication of at least one of Desai’s logs to another of Desai’s filters/templates. For example, Appellants understand Desai’s templates/filters to be applied to data (events described in log copies) after the data has been collected, parsed, normalized and categorized to streamline problem diagnosis (0053-0054). Appellants understand Desai to teach that the filters statistically qualify the data and then compare the findings. In order to compare the findings after statistically qualifying the data, Appellants respectfully submit that Desai would not teach “configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system,” as recited by Claim 1.

RESPONSE TO ARGUMENTS

The Office Action states in the third paragraph under 3.2, “Desai discloses the usage of configured templates for determining whether a message should or should not be processed. (see Desai paragraph [0089] lines 7-9; paragraph

[0093], line 1-3: configuration for analysis).” First, to clarify the record, Appellants respectfully point out that this is a misquotation of Claim 1. Claim 1 recites, “configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template….”

Concerning the reference to Desai’s paragraph 0089 lines 7-11 in section 3.2 of the Office Action, Desai states at lines 7-11 of paragraph 0089,

> Host-based agents can be configured to automatically respond to intrusion attempts before they have a chance to do any damage. Responses might include: (i) kill or reset malicious TCP connections; or (ii) execute any user-defined programs or batch files (emphasis added).

First, Desai states that an automatic response is made which does not qualify as “determining whether data associated with at least one message received by the template should or should not be processed.” Further, “an automatic response is made” (emphasis added) teaches away from “determining whether data…should not be processed.” Appellants respectfully point out that Desai in lines 7-9 of paragraph 0089 goes on to give examples of an automatic response by stating “Responses might include: (i) kill or reset malicious TCP connections; or (ii) execute any user-defined programs or batch files.” Appellants respectfully submit that killing or resetting malicious TCP connections or executing any user-defined programs or batch files does not teach “determining whether data…should or should not be processed…” Appellants understand killing or resetting malicious TCP connections or executing any user-defined programs or batch files to teach away from “determining whether data…should or should not be processed…”

Concerning the reference to Desai’s paragraph 0093 in section 3.2 of the Office Action, Desai states at paragraph 0093,

> Network-based system sensors can be configured to automatically respond to intrusion attempts before they have a chance to do any

> damage. Responses might include: (i) kill or reset malicious TCP connections; (ii) block offending IP address's on firewalls; or (iii) execute any user-defined programs or batch files.

Appellants do not understand Desai's sensors to teach Claim 1's "template" for similar reasons that Appellants do not understand Desai's configured agents (referred to in lines 7-11 of paragraph 0089 quoted and discussed above) to teach Claim 1's "template."

The Office Action goes on to state, "Desai discloses a determination whether a message is acceptable (whether to process) or unacceptable (whether not to process). (See Desai paragraph [0056], lines 1-13…" Desai states at paragraph 0056,

> Any application or service that travels through a security device will have a specific protocol traffic pattern, e.g., HTTP, FTP, Telnet, SQL, etc. Since typical traffic patterns differ across multiple classes or sizes of enterprises, the present invention has established "Customer Traffic Class" categories that set forth "normal" traffic patterns for a given organization's size and network behavior. For greater accuracy in detecting abnormal behavior, and to preclude "false positives", the present invention recognizes protocol traffic patterns based upon an enterprise's business profile (e.g., small office, enterprise, high volume enterprise) before determining whether to classify the event as abnormal behavior.

The Office Action has asserted that Desai's filters/templates teach Claim 1's template. As already described herein, Appellants understand Desai's filters/templates to receive copies of event logs. Appellants understand Desai's filters/templates to analyze logs and to correlate logs in order to determine that there is an unacceptable traffic pattern. Therefore, Appellants do not understand Desai to teach "a determination whether a message is acceptable (whether to process) or unacceptable (whether not to process)" as the Office Action asserts.

Further, it appears to Appellants that there is confusion in the Office Action pertaining to what in Desai is received, what in Desai performs the processing, what in Desai determines whether to process, and what "determination" entails according to Desai’s teachings. For example, Appellants understand Desai to teach the following: Copies of logs are made at devices that for example request Internet services (paragraphs 0043-0046 and Figures 3-4). The copies of the logs are sent and collected on a centralized server in order to analyze and correlate these log copies. Filtering techniques are used as a part of analyzing the copied logs to determine traffic patterns (Figure 5). Further, filtering techniques are used to reduce the number of alarms and to increase the quality of alarms that result from analyzing/correlating the copied logs. Thresholds are applied as part of the filtering techniques to determine traffic patterns. Processing of requests may be modified depending on the result of the traffic pattern determinations (paragraph 0077).

The Office Action states in section 3.3, “Applicant argues, ‘filters cannot be relied on to teach certain features.’ “ This is a misquotation of Appellants’ response. Appellants state that Desai’s filters cannot be relied on to teach certain features of Claim 1‘s template and then Desai’s sensors relied on to teach other features of Claim 1’s template since Appellants understand Desai’s sensors, which sniff the wire (0075) at the devices that create logs as a part of requesting/providing services, to be distinct from Desai’s filters/templates, which are located at a centralized management server (0043) for the purposes of analyzing and correlating copies of logs that were sent to the centralized management server by the devices that created the logs.

The Office Action also states under 3.3, “Desai disclose multiple steps (event analysis engine, event correlation engine, data threshold comparison and analysis) in the analysis of a message.” Appellants respectfully agree.

The Office Action states in section 3.4, “In the event analysis engine, if a threshold is passed, then analysis takes a different path. Events are assigned a severity level and sent to central management server for further analysis and response.” The Office Action indicates that Desai’s threshold processing and analysis are performed before Desai's copies of logs are sent to Desai's centralized server. In contrast, referring to Figure 2, Appellants understand Desai's centralized server to receive and collect copies of logs (81, Figure 2) from various devices such as network devices, firewalls, VPNs, IDSs and Servers, to filter the copies of the logs (82, Figure 2), to perform threshold comparison and analysis which may include assigning a severity (83, Figure 2; 0063), and to perform correlation (85, Figure 2). Further, Appellants understand that if some of Desai's filters/templates did not process some of Desai's logs, then duplicate alarms may result, which is contrary to the intended purpose of Desai to reduce the number of duplicate or false alarms.

The Office Action also states in the second paragraph on page 4, "Additional features performed by the Desai reference do not remove the fact that Desai discloses the configuration of a template and the usage of a template to process messages." First, for the purposes of clarifying the record, Appellants respectfully point out that Claim 1 does not recite "configuration of a template and the usage of a template to process messages. Instead Claim 1 recites,

> configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template;
>
> configuring the template with second information for processing the data associated with at least one of the received messages; and
>
> configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system. (emphasis added)

Second, Appellants respectfully point out that additional features performed by Desai do remove Desai as a candidate for being combined with other references in a future obviousness rejection if those additional features teach away from the embodiment recited by a claim. For example, referring to lines 3-4 of paragraph 0054 and Figure 5, among other things, Appellants understand Desai's templates/filters to process all of Desai's event logs received by a particular template/filter. For at least this reason, Appellants understand Desai to teach away from the embodiment recited by Claim 1.

CONCLUSION

Appellants believe that it is an inherent feature of Desai's filters/templates to always process Desai's logs because if Desai's filters/templates (55) did not always process all of Desai's logs, Desai's logs would not be available for correlation (59) in order to reduce duplicate or false alarms, among other things. Therefore, Appellants do not understand Desai to teach "configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should not be processed by the template."

Appellants do not understand Desai to teach that a single one of Desai's filter/template can be configured with "…first information for determining whether data associated with at least one message…should or should not be processed…," "…second information for processing the data associated with at least one of the received messages…" and "…third information for preventing the communication of at least one received message to other templates…" as recited by Claim 1.

Appellants understand Desai's templates/filters to be applied to data (events described in log copies) after the data has been collected, parsed, normalized and categorized to streamline problem diagnosis (0053-0054). Appellants understand Desai to teach that the filters statistically qualify the data and then compare the findings. In order to compare the findings after statistically qualifying the data, Appellants respectfully submit that Desai would not teach "configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system."

For at least these reasons, independent Claim 1 should be patentable. For similar reasons independent Claims 8 and 14 should also be patentable. Claims 2-7 depend on Claim 1. Claims 9-13 depend on Claim 8. Claims 15-19 depend on Claim 14. These dependent claims include all of the features of their respective independent claims. Further, these dependent claims include additional features which further make them patentable. Therefore, these dependent claims should be patentable for at least the reasons that their respective independent claims should be patentable.

In summary, Appellants respectfully submit that the Office Action's rejections of the claims are improper as the rejection of Claims 1-7 and 14-19 does not satisfy the requirements of a prima facie case of anticipation. Accordingly, Appellants respectfully submit that the rejection of Claims 1-7 and 14-19 under 35 U.S.C. §102(e) are improper and should be reversed.

2. Whether Claims 8-13 are unpatentable under 35 U.S.C. 103(a) in view of Desai (20030188189) and in view of Flowers (6957348)

Appellants have reviewed the cited art and respectfully submit that the embodiments as recited in Claims 8-13 are not taught or suggested by Desai or Flowers, alone or in combination, because of the following rationale.

"As reiterated by the Supreme Court in KSR, the framework for the objective analysis for determining obviousness under 35 U.S.C. 103 is stated in Graham v. John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966). Obviousness is a question of law based on underlying factual inquiries" including "[a]scertaining the differences between the claimed invention and the prior art" (MPEP 2141(II)). "In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious" (emphasis in original; MPEP 2141.02(I)). Appellant notes that "[t]he prior art reference (or references when combined) need not teach or suggest all the claim limitations, however, Office personnel must explain why the difference(s) between the prior art and the claimed invention would have been obvious to one of ordinary skill in the art" (emphasis added; MPEP 2141(III)).

For reasons already provided herein, independent Claims 1 and 14 are patentable over Desai. In additional, Applicants also respectfully submit that Desai teaches away from "configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template," as recited by Claim 1 since Appellants understand Desai to teach that Desai's filters process all of Desai's logs. Appellants also understand Desai to teach away from "configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system," as recited by Claim 1 since Appellants understand that all of Desai's templates would statistically qualify the data in order to compare the findings so that the number of alarms can be reduced and the quality of the alarms would be increased.

For similar reasons, Claim 8 should be patentable over Desai. Flowers does not remedy the deficiency in Desai in that neither Desai nor Flowers, alone or in combination, teach or suggest the embodiment recited by Claim 8. In fact the only part of Claim 8 that the Office Action asserts that Flowers teaches is a guideline. Therefore Claim 8 should be patentable.

Claims 9-13 depend on Claim 8 and include all of the features of Claim 8. Therefore Claims 9-13 should be patentable for at least the reasons that Claim 8 should be patentable.

In summary, Appellants respectfully submit that the Office Action's rejections of the claims are improper as the rejection of Claims 8-13 does not satisfy the requirements of a prima facie case of obviousness as claim features are not met by the cited references. Accordingly, Appellants respectfully submit that the rejection of Claims 8-13 under 35 U.S.C. §103(a) are improper and should be reversed.

In summary, the Appellants respectfully request that the Board reverse the Examiner's rejections of Claims 1-19.

The Appellants wish to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellants' undersigned representative if it is felt that a telephone conference could expedite prosecution.

Respectfully submitted,

WAGNER BLECHER LLP

Date: 3/17/2008 /John P. Wagner, Jr./

John P. Wagner, Jr.

Registration Number: 35,398

WAGNER BLECHER LLP
Westridge Business Park
123 Westridge Drive
Watsonville, CA 95076
408-377-0500

Claims Appendix

1. A method for configuring templates, the method comprising:

configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template;

configuring the template with second information for processing the data associated with at least one of the received messages; and

configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system.

2. The method of Claim 1, wherein configuring the template with second information for processing further comprises configuring the template with the second information for communicating the data associated with at least one of the received messages to a management server.

3. The method of Claim 1, wherein the template is one of an SNMP trap template, a message template, a monitor agent template, a logfile template and a console template.

4. The method of Claim 1, wherein at least one received message is validated with at least one of pattern matching language, MSI, values from environment variables, and values from secure sources.

5. The method of Claim 1, wherein the method further comprises:

configuring the template with fourth information for specifying for a particular received message an action to be performed, wherein the fourth information ensures that the action is performed on a node that generated the particular received message.

6. The method of Claim 1, wherein the second information specifies a superset of conditions for processing all the received messages and wherein:

configuring the template with the first information further comprises configuring the template with the superset of conditions to determine whether data associated with at least one received message should or should not be processed by the template; and

configuring the template with the third information further comprises configuring the template with the superset of conditions to prevent the communication of at least one received message to other templates.

7. The method of Claim 1, wherein the steps of configuring are performed by a template automator.

8. A method for providing a guideline to developers for creating templates, the guideline comprising information used by the developers for:

receiving first information entered by a developer to configure a template of an application and network management system for determining whether data associated with at least one message received by the template should or should not be processed by the template;

receiving second information entered by the developer to configure the template to process the data associated with at least one of the received messages; and

receiving third information entered by the developer to configure the template to prevent the communication of at least one received message to other templates of the application and network management system.

9. The method of Claim 8, wherein second information to process the data further comprises the second information to communicate the data associated with at least one of the received messages to a management server.

10. The method of Claim 8, wherein the template is one of an SNMP trap template, a message template, a monitor agent template, a logfile template and a console template.

11. The method of Claim 8, wherein at least one received message is validated with at least one of pattern matching language, MSI, values from environment variables, and values from secure sources.

12. The method of Claim 8, wherein the method further comprises:

receiving fourth information entered by the developer to configure the template to specify an action for a particular received message, wherein the fourth information ensures that the action is performed on a node that generated the particular received message.

13. The method of Claim 8, wherein the second information specifies a superset of conditions for processing all the received messages and wherein:

receiving the first information further comprises configuring the template with the superset of conditions to determine whether data associated with at least one received message should or should not be processed by the template; and

receiving the third information further comprises configuring the template with the superset of conditions to prevent the communication of at least one received message to other templates.

14. A computer system comprising:

a memory unit; and

a processor coupled to the memory unit, wherein the processor executes instructions associated with a template automator, and wherein the instructions of the template automator are for:

configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template;

configuring the template with second information for processing the data associated with at least one of the received messages; and

configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system.

15. The method of Claim 14, wherein configuring the template with second information for processing further comprises configuring the template with the second information for communicating the data associated with at least one of the received messages to a management server.

16. The computer system of Claim 14, wherein the template is one of an SNMP trap template, a message template, a monitor agent template, a logfile template and a console template.

17. The computer system of Claim 14, wherein at least one received message is validated with at least one of pattern matching language, MSI, values from environment variables, and values from secure sources.

18. The computer system of Claim 14, wherein the template automator further comprises instructions for:

configuring the template with fourth information for specifying for a particular received message an action to be performed, wherein the fourth information ensures that the action is performed on a node that generated the particular received message.

19. The computer system of Claim 14, wherein the second information specifies a superset of conditions for processing all the received messages and wherein:

configuring the template with the first information further comprises configuring the template with the superset of conditions to determine whether data associated with at least one received message should or should not be processed by the template; and

configuring the template with the third information further comprises configuring the template with the superset of conditions to prevent the communication of at least one received message to other templates.

Evidence Appendix

None

Related Proceedings Appendix

None